Logistics Management Institute

Defense Transportation's EDI Program: A Security Risk Assessment

PL205LN5

May 1993

Harold L. Frohman
William R. Ledder

Prepared pursuant to Department of Defense Contract MDA903-90-C-0006. The views expressed here are those of the Logistics Management Institute at the time of issue but not necessarily those of the Department of Defense. Permission to quote or reproduce any part except for Government purposes must be obtained from the Logistics Management Institute.

Logistics Management Institute
6400 Goldsboro Road
Bethesda, Maryland 20817-5886

CONTENTS

DEFENSE TRANSPORTATION'S EDI PROGRAM: A SECURITY RISK ASSESSMENT

INTRODUCTION

The Computer Security Act of 1987 requires that "each Federal agency shall... establish a plan for the security and privacy of each Federal computer system... that is commensurate with the risk and magnitude of the harm resulting from the loss, misuse, or unauthorized access to or modification of the information contained in such system." This report details how the Department of Defense (DoD) has responded to the provisions of that act in the design and development of its electronic data interchange (EDI) program for transportation.

BACKGROUND

In 1989, the General Services Administration (GSA) amended Title 41 Code of Federal Regulations (CFR), Part 101-41, "Federal Property Management Regulations" to permit Federal agencies to electronically transmit carrier billings and backup documentation for freight and personal property transportation services as an alternative to issuing the hard copy Standard Forms (SFs). This amendment authorizes DoD to use EDI techniques to document and pay transportation bills, replacing a number of paper forms such as the Government bill of lading (GBL) and public vouchers.

The DoD's EDI program for transportation calls for more than 160 DoD shipping activities, the Military Traffic Management Command (MTMC), Defense finance centers, GSA, and commercial carriers to design and develop EDI systems that ensure the timely and accurate flow of information. Each of those EDI systems is required to comply with the provisions of the following documents:

- DoD Directive 5200.28, *Security Requirements for Automated Information Systems (AISs)*, 21 March 1988

- Federal Managers' Financial Integrity Act and Internal Management Control Program, which are mandated by Office of Management and Budget (OMB) Circular A-123, "Internal Control Systems," 4 August 1986
- DoD Document No. CSC-STD-002-85, "DoD Password Management Guideline," 12 April 1985.

The introduction of EDI in Defense transportation requires a number of changes to business procedures and internal controls. Those changes also introduce new security risks. We believe that Defense transportation's EDI program, particularly in the payment process, is designed to meet or exceed the security measures embedded in the existing paper environment. Before describing those measures and the DoD's response to them, we provide an overview of the DoD's EDI operating concept.

DEFENSE TRANSPORTATION'S EDI OPERATING CONCEPT

The DoD's concept for electronically linking its shipping activities and finance centers, MTMC, GSA, and commercial trading partners involves three separate processes: GBL generation and distribution, prepayment auditing and payment processing, and postpayment auditing.

A Defense shipping activity generates a GBL using an automated system. The activity gives the original paper GBL to the commercial carrier's driver to serve as an intransit manifest to satisfy Federal and State commerce and safety regulations and as proof of service; it also retains a signed paper copy of the GBL to serve as contractual evidence. The activity transmits the shipment information contained on the GBL to the carrier, all consignees, and MTMC using the American National Standards Institute (ANSI) Accredited Standards Committee (ASC) X12 Transaction Set 858, *Shipment Information*.

Upon receipt of the shipment information, MTMC verifies that a valid tender exists for the carrier. If a tender does not exist, MTMC rejects the shipment in a message that it sends electronically to the originating shipping activity. Otherwise, MTMC creates an electronic record of the shipment and makes that shipment information available to DoD finance centers, as requested. In addition, MTMC either determines the cost of each shipment or provides tender information to the appropriate DoD finance center, which uses that information to rate the shipment.

Commercial carriers transmit invoices electronically to DoD finance centers, also using the ASC X12 standards. (This practice is in contrast to the current paper environment in which carriers submit both the original paper GBL and public voucher.) The finance center then audits the electronic invoice prior to payment by matching the rated shipment information received from MTMC with the appropriate invoice and reconciling any differences. If a matching shipment information record cannot be located, MTMC electronically queries the originating shipping activity for that record. The shipping activity determines whether the shipment is valid and transmits an electronic message back to MTMC. If the shipment is not valid, the finance center requires the carrier to submit paper documentation to substantiate the invoice in order to receive payment.

Following the match and reconciliation process, the finance center will pay the amount on the shipment information record or on the invoice (whichever is lower), using either paper checks or electronic funds transfer to the carrier's bank. The finance center next completes the record for that shipment by sending payment information to MTMC; it also sends shipment and invoice information to GSA for postpayment audit, using the ASC X12 Transaction Set 820, *Remittance Advice.*

Figure 1 presents a schematic of this operating concept. One of the keys to this concept is the use of an EDI value-added network (VAN). Such a VAN facilitates the exchange of EDI-formatted information between DoD activities and commercial carriers. In addition, most DoD shipping activities will use an EDI VAN to send shipment information to MTMC. Figure 2 shows the role of EDI VANs in Defense transportation's EDI program. (Because of the volume of information transmitted among MTMC, GSA, and DoD finance centers, the use of leased lines is more economical than an EDI VAN.)

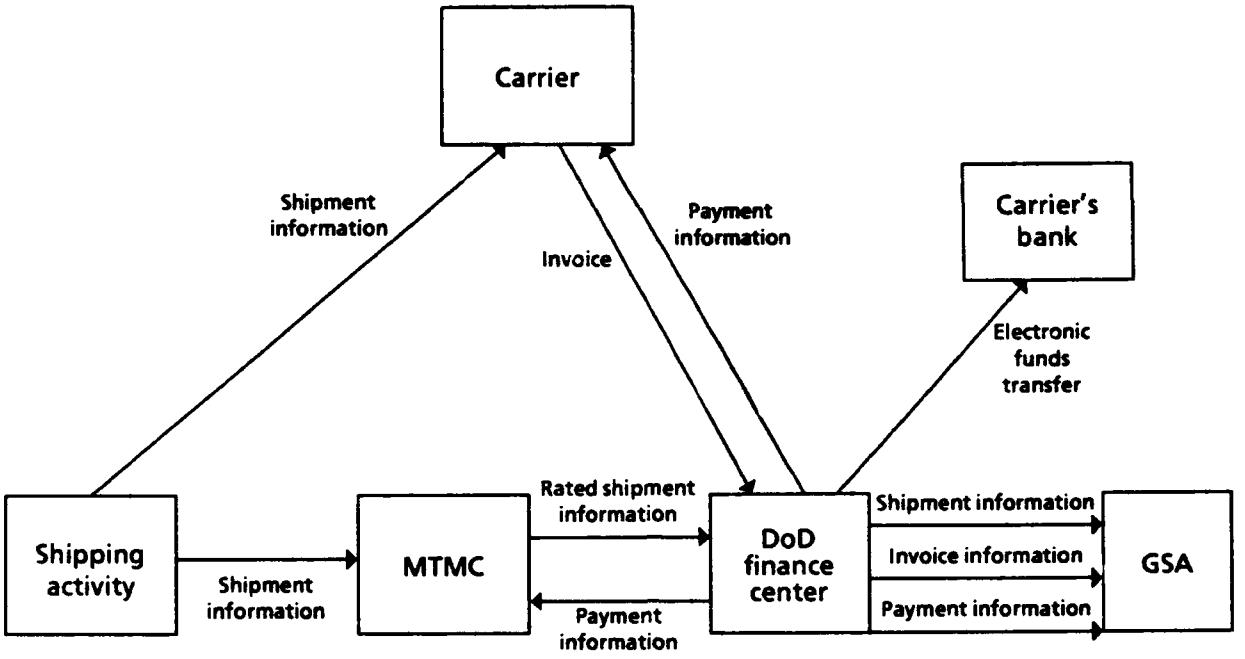

FIG. 1. DEFENSE TRANSPORTATION'S EDI OPERATING CONCEPT

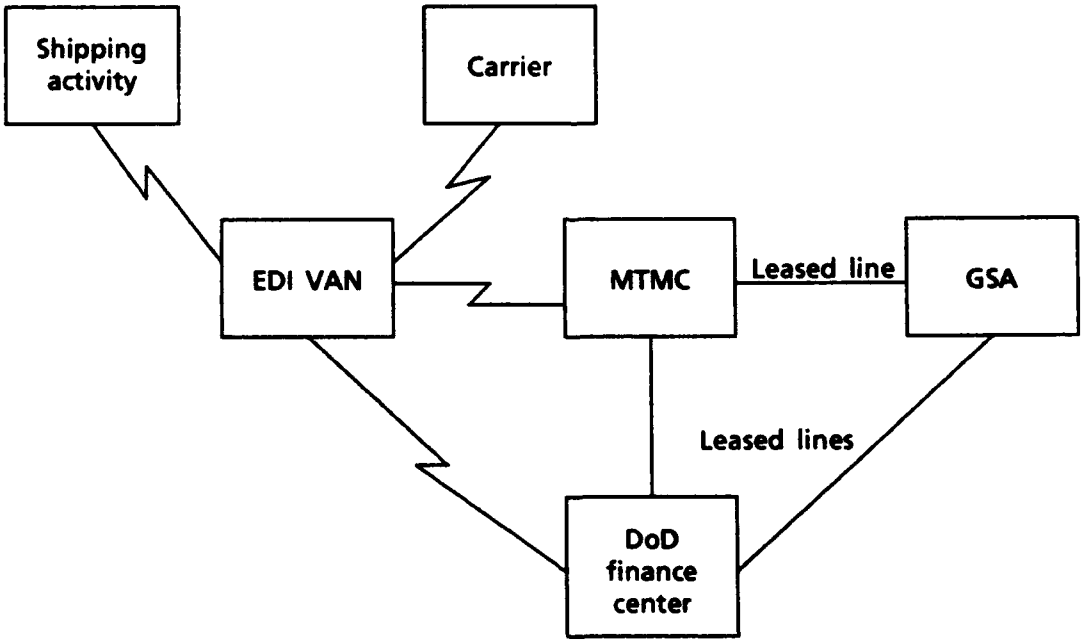

FIG. 2. EDI TELECOMMUNICATIONS

ASSESSMENT FINDINGS

In this section, we examine the Computer Security Act requirements for defining the sensitivity of Defense transportation data. (Those requirements are important because the data security measures in an EDI program must be commensurate with the level of risk assigned to each data type.) We then describe how Defense transportation's EDI program satisfies the four key security guidelines suggested by the National Institute of Standards and Technology (NIST). Finally, we discuss how Defense transportation's internal financial controls operate in unison with EDI security techniques to provide end-to-end protection of transportation data.

Sensitivity of Transportation Data

The types of data in Defense transportation's EDI program should be categorized according to their level of risk in order to determine the appropriate data security measures. The Computer Security Act defines sensitive, but unclassified information, as

> . . . any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of Federal programs, or the privacy to which individuals are entitled under section 552a of title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive order or an Act of Congress to be kept secret in the interest of national defense or foreign policy. . . .

Table 1 lists several types of sensitive data, defines each type, and provides representative examples. According to the criteria presented in that table, electronically transmitted transportation documents such as GBLs and commercial invoices should be treated as sensitive because they contain vital records information (i.e., information that DoD needs to function normally). Other EDI transportation transactions, such as shipment status messages, do not contain that information so they are considered nonsensitive.

TABLE 1

TYPES OF SENSITIVE DATA

Type	Definition	Example
Vital records	Records essential to maintaining continuity of Government activities during a national emergency	• Emergency operation records • Rights and interest records
Privacy Act information	Records maintained on an individual that include a name, identifying number, symbol, or other particulars assigned to an individual	• Payment and retirement records • Medical and psychological records • Educational achievement records • Financial records
Official use only	Unclassified information that may be exempt from public release under the Freedom of Information Act	• Internal correspondence • Working papers
National security related	Unclassified information that alone or in the aggregate, reveals information regarding a high-volume U.S. program or initiative	• Unclassified intelligence information • Controlled scientific and technical information • Foreign exchange information
Security management	Unclassified information developed and stored to administer and ensure compliance with security programs	• Limited access information • Security/internal audit information • Legal information
Commercial information	Unclassified information that, if released, could provide unfair advantage to competitors	• Contract or proprietary information

Source: Julie A. Smith, Logistics Management Institute, "EDI Risk Assessment Methodology for Unclassified/Sensitive Information," presented at the Workshop on Security Procedures for the Interchange of Electronic Documents, NIST, 12 – 13 November 1992.

Sensitive data can also be further categorized according to three levels of risk:[1]

- *Low-risk applications*, which offer little incentive for tampering by third parties; examples include invoices, bills of lading, and small purchase transactions

[1]Peter N. Weiss, Office of Management and Budget, "Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Toward Developing a Security Policy." Presented at the Workshop on Security Procedures for the Interchange of Electronic Documents, NIST, 12 – 13 November 1992.

- *Medium-risk applications*, which present significant incentives for tampering and/or which require a reasonable level of confidentiality; examples include responses to invitations for bid and requests for proposals
- *High-risk applications*, where message confidentiality is of particular concern or a lack of message integrity presents great risk, and the access controls are inadequate; electronic funds transfer transactions satisfy these criteria.

We believe that the sensitive EDI transactions in Defense transportation's program are in the low-risk category because they do not require a high degree of confidentiality and they present little incentive for tampering by a third party.

EDI Security Policy

The Computer Security Act also assigns NIST the responsibility for developing security standards and guidelines for all sensitive data, including data transmitted using EDI. Although NIST has not formally issued an EDI security policy, it has published a bulletin that describes the Government's security requirements and some of the corresponding security techniques that Federal agencies could incorporate into their EDI applications.[2]

We believe that this bulletin eventually will serve as the primary input to a Federal Information Processing Standards publication describing EDI security. As a result, we use its provisions as a basis for assessing the security measures in Defense transportation's EDI program.

Security Measures

The June 1991 CSL bulletin identifies four security requirements of specific concern to EDI systems: confidentiality, message integrity, authentication and nonrepudiation, and (systems) availability. It also discusses the requirements for maintaining electronic records.

In the remainder of this report, we describe those requirements in some detail and Defense transportation's means for satisfying them. Table 2 identifies several techniques for ensuring the security of EDI transactions, with those used to protect

---

[2]Computer Systems Laboratory (CSL) Bulletin, "Security Issues in the Use of Electronic Data Interchange," June 1991, NIST.

the least sensitive data at the top (which approximates DoD's situation).[3] Although the table does not show the availability requirement, we discuss it under the systems availability category. Finally, we provide an overview of electronic records management and how Defense transportation meets Federal requirements for such management.

TABLE 2

EDI SECURITY REQUIREMENTS AND TECHNIQUES

Security technique	Requirement			
	Confidentiality	Message integrity	Originator authentication	Nonrepudiation
Access controls	X		X	X
Embedded references			X	X
Functional acknowledgment			X	X
Message repetition acknowledgment		X	X	X
Internal message verification		X		
Trusted third party	X	X	X	X
Cryptographic data authentication		X	X	X
Data encryption	X			X

Source: Peter Weiss, "Security Requirements and Evidentiary Issues in the Interchange of Electronic Documents: Steps Towards Developing a Security Policy." Presented at the Workshop on Security Procedures for the Interchange of Electronic Documents, National Institute of Standards and Technology, 12 – 13 November 1992.

Confidentiality

Confidentiality refers to the need to restrict sensitive information from being disclosed to unauthorized recipients. For example, EDI transactions may contain

[3]Defense transportation does not use several of the techniques listed in the table: message repetition acknowledgment, where the recipient of a message acknowledges receipt by repeating back its full contents; internal message verification, where certain message fields are summed in a hash total for recalculation and verification by the recipient of the message; cryptographic data authentication, where secret encryption keys are used to calculate digital signatures or similar authentication signatures; and data encryption, where encryption keys are used to secretly code all elements of a message. These techniques are typically used for data categorized as either medium or highly sensitive.

personal data, sensitive financial information, or other data that must be treated as confidential.

As a means of controlling access to EDI systems, DoD shipping activities and finance centers, MTMC, and the EDI VAN all employ unique character strings (user identification codes) and passwords to identify authorized system users. Those passwords must be created and maintained in accordance with the guidelines and provisions of DoD Document No. CSC-STD-002-85, "DoD Password Management Guideline," 12 April 1985. However, we were unable to determine the degree of compliance with that document by all DoD shipping activities. In addition, the DoD's commercial trading partners are required to complete and sign a trading partner agreement.[4] That agreement defines some of the security mechanisms that they need to implement and binds them to the requirements of numerous Federal and DoD documents and regulations. The agreement also stipulates that "... Under no circumstances shall a trading partner sell or trade any shipment information for purposes other than those associated with providing the requested transportation services...."

We believe that the use of access controls and trading partner agreements provide adequate data confidentiality in Defense transportation's electronic environment.

Message Integrity

Data or message integrity is defined in OMB Bulletin No. 90-08, "Guidance for Preparation of Security Plans for Federal Computer Systems that Contain Sensitive Information," 9 July 1990, as "... information which must be protected from unauthorized, unanticipated or unintentional modification, including the detection of such activities...."

As Table 2 indicates, some degree of message integrity is provided by using a trusted third party, such as an EDI VAN, to exchange EDI transactions between trading partners. In addition to its access controls and physical security measures, an EDI VAN provides message status reports, message filing and audit trail services,

---

[4]LMI Report PL205LN2, *EDI Trading Partner Agreement for Defense Transportation: Freight*, W. Michael Bridges, Harold L. Frohman, William R. Ledder, and Theresa Yee, March 1993.

as well as other security services. (See the appendix for further details on a trusted third party.)

We believe that use of an EDI VAN in combination with the access control measures satisfies NIST's message integrity guidelines.

Originator Authentication and Nonrepudiation

Originator authentication of EDI transactions ensures that the recipient of an electronic message knows that the source of the message is the named originator, not some other entity. Nonrepudiation, a stronger form of authentication, ensures that one of two parties to an electronic transmission cannot falsely deny involvement in a transaction. However, nonrepudiation is not applicable to the DoD's EDI transportation program because it is unlikely that a carrier will deny submitting an invoice to the payment center.

The DoD has implemented in its transportation payment program many of the security techniques in Table 2 that provide authentication. The access controls, which we described under confidentiality, provide a degree of originator authentication. The embedded references are numbers or passwords that two parties agree to use. Defense transportation employs two forms of those references. The first, EDI sender and receiver codes (i.e., ASC X12 identification codes), is embedded within the ANSI X12 interchange control envelope that the EDI VAN uses to address groups of transactions. (The appendix describes how DoD and an EDI VAN use sender and receiver codes for security purposes.)

The second form of embedded reference is a requirement in the DoD's trading partner agreement. Each shipping activity is required to submit a discrete authenticating code in the N406 segment of Transaction Set 858, *Shipment Information*. In addition, each carrier is required to submit a payee code in the N902 segment of all invoices submitted electronically to a finance center. Those authenticating codes, along with the transmission of the appropriate transaction set, represent the equivalent of a signature.

Transaction Set 997, *Functional Acknowledgment*, which notifies the originator of an EDI transmission that it has been accepted or rejected, provides another level of originator authentication. The trading partner agreement requires that all parties send a functional acknowledgment by the close of the following business day after

receiving an EDI transaction, such as a GBL or an invoice. (If the originator does not receive an acknowledgment in the prescribed time period, it is the originator's responsibility to determine if a problem exists.)

Finally, the use of an EDI VAN as a trusted third party provides additional originator authentication. Only authorized users can access the EDI VAN to retrieve or deposit EDI transactions from or to a particular EDI mailbox.

We believe that Defense transportation's EDI program provides sufficient originator authentication to meet Federal guidelines for data categorized as having low sensitivity.

Systems Availability

According to OMB Bulletin No.90-08, EDI information "... must be available on a timely basis to meet mission requirements or to avoid substantial losses." Thus, automated system failures would likely delay Defense transportation operations. As a consequence, DoD activities need to develop contingency plans and the associated backup and recovery procedures to satisfy their immediate operating concerns. They are to prepare and test those plans in accordance with the guidelines and provisions of OMB Bulletin 90-08 and Appendix III, OMB Circular No. A-130 "Management of Federal Information Resources," 12 December 1985. The finance centers and MTMC are currently developing their contingency plans and upon completion, will be required to test them. In addition, the finance centers and MTMC archive their EDI transactions after the EDI translation software processes them. Only authorized users are permitted to access that archived data and each access is logged. Because the EDI VAN also archives EDI transaction data, the finance centers are exploring the use of that service for backup procedures. Finally, DoD shipping activities are required to archive their EDI transactions, in addition to retaining a copy of the original paper GBL that they provided to the commercial carrier.

Because all DoD systems are required to comply with the provisions of those documents, DoD's EDI transportation systems also must satisfy OMB's availability requirements.

Electronic Records Management

Transportation information must be retained for a period of time after usage to fulfill Federal record retention, legal, and audit requirements. The creation, use,

preservation, and disposition of electronic records is mandated in Title 36 CFR Part 1234, "Electronic Records Management," by the National Archives and Records Administration.

In this section, we examine three primary issues associated with the management of electronic records: controlling access to electronic records, maintaining proper audit trails, and providing for backup and recovery. We also discuss the use of electronic records as evidence in Federal courts.

Controlling Access. Defense transportation's EDI program uses several methods for controlling access to sensitive records. In compliance with DoD Directive 5200.28, all DoD activities are required to restrict physical access to their computer rooms. Most shipping activities, for instance, require card keys for entrance into their computer rooms. All activities, including shippers, MTMC, and payment centers, use passwords to prevent unauthorized users from accessing their transportation systems. In addition, computer system administrators grant permission to access sensitive records only to authorized personnel.

Maintaining Audit Trails. Audit trails are another important aspect of electronic records management. They are primarily provided by the EDI VAN, which maintains records of who deposited or received certain data and when that activity occurred.

Provides Backup and Recovery. The backup and recovery of electronic transportation records protects against information loss and ensures that the records are available for later use. Because backup and recovery is addressed in systems availability and the EDI VAN backs up all the records it processes, we believe that Defense transportation systems fully satisfy the requirements of Title 36 CFR.

Judicial Use of Electronic Records. Title 36 CFR also states that electronic records may be admitted as evidence in court if the system containing the records has documented and trustworthy controls that prevent unauthorized addition, modification, or deletion of data. The records must also be available when needed.

One way to provide proof of system-security procedures is to follow the guidelines in the Internal Management Control Program (IMCP), as mandated by the Federal Manager's Financial Integrity Act (FMFIA). The IMCP prescribes both general and specific standards for maintaining appropriate internal controls. For

example, the IMCP states that control systems shall be properly documented, transactions and other significant events promptly recorded, transactions and other significant events authorized and executed only by appropriate persons, and "key duties and responsibilities in authorizing, processing, recording, and reviewing transactions shall be separated among individuals."

We believe that given its security procedures and use of an EDI VAN as a trusted third party, Defense transportation's EDI program meets most Federal electronic records management requirements. Implementation of an IMCP or similar internal controls review program that addresses EDI security controls would fulfill the remaining requirements.

Internal Controls

To provide adequate protection of sensitive data, EDI security techniques must operate in parallel with internal financial controls. The June 1991 CSL bulletin states "... certain types of messages may be more inherently sensitive than other types. Less care would need to be taken with an invoice sent to an agency, if the agency's internal control system is sufficiently robust so that it would reject all non-authentic invoices...." We believe that Defense transportation has implemented an appropriate series of controls to protect its payment systems against duplicate invoices, incorrect charges, unauthorized services, falsely submitted invoices, unauthorized payments, and other transgressions. Those controls, which we described briefly in the operating concept, consist of

- An invoice submitted by a carrier to a finance center must match a corresponding shipment information transaction submitted by MTMC.
- The payment center pays the lower of the invoice or shipment record amounts.
- All shipments are authorized by a DoD shipping activity through the submission of an electronic shipment information record.
- All shipment information records are validated, edited, and rated by MTMC prior to matching with an invoice at a finance center.

SUMMARY AND CONCLUSION

The DoD is building upon private-sector experiences in using EDI techniques to pay commercial carriers for their services. In developing such a capability, DoD has

many of the same security requirements of private-sector companies that routinely exchange shipment and invoice information with their commercial carrier trading partners. We conclude that the security measures and internal controls used in the DoD's EDI program are appropriate for the level of risk involved and provide adequate protection to the Government for the areas we examined. Those measures and controls include the authorization of shipments by DoD shipping activities; matching of carrier invoices to shipment information received from DoD shipping activities; extensive use of access controls, discrete authenticating codes, unique EDI sender and receiver codes and functional acknowledgments; availability of backup documentation in paper form; and compliance with the provisions of DoD Directive 5200.28, FMFIA, OMB Circular A-123, and OMB Bulletin 90-08.

Because we did not fully assess password management at all Defense transportation activities, each activity must be certain it complies with DoD Document No. CSC-STD-002-85. In addition, systems availability requirements will be fully met when MTMC and the finance centers finish developing and testing their contingency plans in accordance with OMB Bulletin 90-08. Finally, each Defense transportation activity needs to verify that they have implemented an internal control systems review that addresses EDI security controls in order to fully satisfy electronic records management requirements.

APPENDIX

SECURITY TECHNIQUES

This appendix further explains some of the security techniques incorporated into Defense transportation's electronic data interchange (EDI) program.

BACKUP DOCUMENTATION

Backup documentation consists of the original paper Government bill of lading (GBL) that the carrier uses to substantiate an electronic invoice.

EDI SENDER AND RECEIVER CODES

The EDI sender and receiver codes are American National Standard Institute (ANSI) Accredited Standards Committee (ASC) X12 identification codes within the ANSI X12 interchange envelope that are assigned to specific trading partners. The use of EDI sender and receiver codes ensures that the recipient of an electronic message knows that the source of the message is the named originator.

The EDI value-added network (VAN) maintains a table of sender and receiver codes and the transaction sets that all receivers will accept from a particular sender. For example, if a sender transmits a transaction set to the Military Traffic Management Command's (MTMC's) EDI mailbox, the transmission will be deposited only if MTMC had previously identified the sender and the specific ASC X12 transaction set as acceptable. Otherwise, the EDI VAN discards the transaction set but logs the information in its audit trail.

In addition, MTMC's EDI translation software and that of the Department of Defense (DoD) finance centers validate the sender's identification code prior to processing any information received from a carrier or other DoD activity.

DISCRETE AUTHENTICATING CODE

A discrete authenticating code, which is known only to the EDI sender and receiver, is placed by the sender in a specified data element within the transaction set. That code functions as a private password between the sender and receiver. The

payee code in the invoice and the GBL Office Code serve as the discrete authenticating codes.

FUNCTIONAL ACKNOWLEDGMENT

The DoD requires that each trading partner electronically send a confirmation message to the sender every time it receives a message. In addition, the trading partner agreement, which is executed between DoD and the carrier, requires that DoD activities transmit an ASC X12 Transaction Set 997, *Functional Acknowledgment*, within 1 business day of receipt of a transmission from a carrier.

INTERNAL FINANCIAL CONTROLS

Internal financial controls are integral to Defense transportation's EDI program. They are designed to meet or exceed the security measures in place for paper documents and to be commensurate with the associated level of risk.

PHYSICAL SECURITY

Each automated system in Defense transportation's EDI program is required to comply with the security requirements prescribed by DoD Directive 5200.28, "Security Requirements for Automated Information Systems (AISs)," 21 March 1988, particularly those that address physical (hardware), personnel, and industrial security.

SHIPMENT AUTHORIZATION

The transportation officer at each shipping activity is responsible for all shipment information disseminated by that activity. In addition, a budget officer is ultimately responsible for all transportation charges incurred at a shipping activity and any excess or extraordinary charges (e.g., charges for services that were not performed).

TRUSTED THIRD PARTY

The use of a trusted third-party service provider (i.e., the EDI VAN) provides another layer of security for Defense transportation data. The EDI VAN uses originator authentication and access controls, including log-on procedures, user passwords, and ANSI X12 identification codes, to protect the data on its system and ensure that the data sent to an EDI mailbox retains its integrity. The EDI VAN also maintains audit trails and security logs that document data modifications and

monitor access to mailboxes. Finally, the EDI VAN provides status reports that detail the specific transmission interchange control numbers that it processed, transaction types exchanged between a sender and receiver, date and time stamps, and other information that could be used to document that a sender/receiver pair exchanged information.

REPORT DOCUMENTATION PAGE

Form Approved
OPM No. 0704-0188

1. AGENCY USE ONLY *(Leave Blank)*	2. REPORT DATE	3. REPORT TYPE AND DATES COVERED
	May 93	Final

4. TITLE AND SUBTITLE
Defense Transportation's EDI Program: A Security Risk Assessment

5. FUNDING NUMBERS
C MDA903-90-C-0006
PE 0902198D

6. AUTHOR(S)
Harold L. Frohman and William R. Ledder

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Logistics Management Institute
6400 Goldsboro Road
Bethesda, MD 20817-5886

8. PERFORMING ORGANIZATION REPORT NUMBER
LMI-PL205LN5

9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)
Office of the Secretary of Defense (Production and Logistics)
The Pentagon
Room 3E808
Washington, DC 20301-8000

10. SPONSORING/MONITORING AGENCY REPORT NUMBER

11. SUPPLEMENTARY NOTES

12a. DISTRIBUTION/AVAILABILITY STATEMENT
A: Approved for public release; distribution unlimited

12b. DISTRIBUTION CODE

13. ABSTRACT *(Maximum 200 words)*

As the Department of Defense (DoD) implements electronic data interchange (EDI) techniques to replace documents in its transportation processes, security issues must be addressed. This report describes Defense transportation's EDI operating concept and the current Federal and DoD security laws, guidelines, and documents that are applicable to EDI programs. The security measures and internal controls implemented in Defense transportation's EDI program are also documented.

14. SUBJECT TERMS
EDI; electronic data interchange; transportation; electronic invoicing; security; shipment information; Transaction Set 858; ASC X12 858

15. NUMBER OF PAGES
20

16. PRICE CODE

17. SECURITY CLASSIFICATION OF REPORT	18. SECURITY CLASSIFICATION OF THIS PAGE	19. SECURITY CLASSIFICATION OF ABSTRACT	20. LIMITATION OF ABSTRACT
Unclassified	Unclassified	Unclassified	UL